



Bundaberg Christian College  
Education with Wisdom

# BCC

# Acceptable Use

# of ICT Policy

“EDUCATION WITH WISDOM”

“**Wisdom** is supreme; therefore get wisdom. Though it cost all you have, get **understanding**.”

(Proverbs 4:7)

Version 1.0

Updated Last: 31/07/2024

Review Date: 01/07/2026

**Respect | Integrity | Servanthood | Excellence**

P (07) 4132 5800 E [info@bcc.net.au](mailto:info@bcc.net.au) W [www.bcc.net.au](http://www.bcc.net.au)  
234 Ashfield Road Bundaberg QLD 4670

# **Contents**

|  |   |
|--|---|
| <i>PURPOSE</i> .....   | 3 |
| <i>SCOPE</i> .....   | 3 |
| <i>REFERENCES</i> .....  | 3 |
| <i>DEFINITIONS</i> .....   | 3 |
| <i>General Principles</i> .....  | 4 |
| <i>Online Conduct</i> .....  | 4 |
| <i>Access and Authorisation</i> .....                                  | 4 |
| <i>Data Security and Privacy</i> .....                                 | 4 |
| <i>Online Communication and Behaviour</i> .....                        | 5 |
| <i>Content Creation</i> .....  | 5 |
| <i>Use of Artificial Intelligence (AI)</i> .....                       | 5 |
| <i>Network and Internet Use</i> .....                                  | 5 |
| <i>Personal Device Use</i> .....                                       | 5 |
| <i>Use of School Identity</i> .....                                    | 6 |
| <i>Consequences of Violation</i> .....                                 | 6 |
| <i>Resources and Support</i> .....                                     | 6 |
| <i>Appendix 1: Cybersecurity Guidelines</i> .....                      | 7 |
| <i>Appendix 2: Acceptable Use of ICT Policy: Student Version</i> ..... | 8 |

## **PURPOSE**

The purpose of this policy is to establish clear expectations and guidelines for the responsible, ethical, and secure use of all ICT resources within Bundaberg Christian College (BCC), including school-owned ICT resources as well as personal ICT devices when they are used for school-related activities.

## **SCOPE**

This policy applies to all users of ICT at BCC, including staff, students, volunteers, authorised guests, and contractors.

## **REFERENCES**

*Privacy Act 1988 (Cth)*

*Copyright Act 1968 (Cth)*

*Australian Privacy Principles*

*The Australian Student Wellbeing Framework*

*National Principles for Child Safe Organisations*

*Australian Framework for Generative Artificial Intelligence in Schools*

*eSafety Toolkit for Schools*

*Queensland Government Department of Education Use of ICT systems procedure*

*BCC Student Code of Conduct*

*BCC Student Laptop Policy*

*BCC Staff Code of Conduct*

*BCC Privacy Policy including Data Breach Response Plan*

*BCC Records Retention Policy*

*BCC Formal Complaints Policy and Procedures*

## **DEFINITIONS**

- **Acceptable use:** The use of technology aligning with the values and purposes of BCC and the intent of this policy, complying with relevant laws and regulations, and respecting the rights of others.
- **AI tools:** Computer programs utilising machine learning algorithms and other advanced techniques to mimic human cognitive abilities like reasoning, pattern recognition, and learning from data. These tools can generate creative content, assist with problem-solving, and automate certain tasks.
- **Copyright:** Legal protection granted to original creative works.
- **Cyberbullying:** Repeated online harassment or intimidation targeting an individual.
- **Data:** Any information stored or transmitted electronically, including personal or sensitive information of students and staff.
- **ICT (Information and Communication Technology):** Refers to all technology provided by BCC used for collecting, storing, processing, transmitting, and communicating information, including computers, networks, software, applications, and internet access, and personal devices used for school-related activities.
- **Network resources:** Hardware and software infrastructure supporting BCC's technology network.
- **Personal device:** Any electronic device owned by a user that is brought to school or used for school-related activities, such as laptops, phones, tablets, smartwatches, etc.
- **Plagiarism:** Using someone else's work or ideas without conferring appropriate credit.
- **School-related activities:** Any activity connected to the College's services, including administration, operations, classes, breaks, assignments, clubs, extracurricular activities, school trips, and online communication of staff, teachers and students.
- **User:** Any individual authorised to use BCC's ICT, including staff, students, volunteers, authorised guests, and contractors.

## General Principles

1. All ICT use must be responsible, ethical, and legal, respecting the rights and dignity of others.
2. ICT should be used to support learning, communication, and collaboration within the school community.
3. ICT should be used in a way that maintains a safe and productive learning environment for all.
4. To ensure the responsible and safe use of the College's network, BCC reserves the right to monitor and maintain appropriate records of network activity using a range of approved methods and platforms (e.g., email, web browsing, file sharing). This monitoring is conducted in alignment with applicable laws to protect the school community and maintain a secure learning environment.

## Online Conduct

- Using ICT to engage in any illegal activity, such as hacking, accessing or distributing illegal content, or participating in online scams, under any circumstances, is strictly prohibited.
- Users must not engage in any online behaviour that is intended to intimidate, humiliate, threaten, or harass another person, including sending offensive messages, excluding others from online groups with the intent to ostracise, spreading false or harmful information, or impersonating others.
- Sharing content online that is hateful, discriminatory, promotes violence or illegal activities, or expresses discriminatory views based on protected characteristics such as race, religion, gender, sexual orientation, disability, or any other personal attribute is strictly prohibited.
- Users must not engage in activities that violate community standards of decency and professionalism regarding online content. This includes accessing, viewing, or distributing materials of a sexually suggestive or exploitative nature.

## Access and Authorisation

- Access to school technology is granted on a privilege basis and for approved school and work-related purposes only.
- Limited personal use of school technology may be permitted for staff members during off-duty hours and within the acceptable use parameters outlined in this policy, as long as it doesn't interfere with official duties and incur more than negligible costs.
- Downloading and installing unauthorised software using school technology, including games, gambling software, pirated software, or applications that bypass school security measures or disrupt network performance, is strictly prohibited.
- Users must only access school technology using their own authorised accounts. Sharing of authorised accounts or passwords is **strictly prohibited**.
- Accessing data or systems that users are not authorised or directed to access, as part of their employment, or attempting to bypass security measures to gain unauthorised access is strictly prohibited.
- Users must not share confidential information with unauthorised individuals or organisations.

## Data Security and Privacy

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- Unauthorised enrolment, sign-up or subscription of applications or platforms, is strictly prohibited and requires approval by the College (Head of School, Faculty or Department).
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures, such as those detailed within this policy, to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with the *BCC Privacy Policy* and Data Breach Response Plan.
- Multi-factor authentication is mandatory for all staff accessing school systems and networks.

## Online Communication and Behaviour

- All online communication must be respectful, courteous, and professional.
- Cyberbullying, harassment, and discrimination are strictly prohibited.
- Users must not engage in offensive or illegal online activities.

## Content Creation

- Users must respect copyright laws, avoid plagiarism, and not use ICT in any way that impacts on the academic integrity of work produced.
- Using copyrighted materials without permission, such as downloading or sharing music, movies, software, or other copyrighted works without the owner's consent is strictly prohibited.
- Submitting work that is plagiarised is strictly prohibited.

## Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) at BCC must be used in a manner consistent with the ethical and educational principles outlined in the [\*Australian Framework for Generative Artificial Intelligence in Schools\*](#). AI tools should enhance learning, streamline administrative tasks, and foster innovation while adhering to BCC's values of respect, integrity, and transparency. Users are expected to ensure that AI applications respect privacy, promote inclusivity, and do not perpetuate bias or discrimination. All AI systems must be transparent in their operations and decisions, with appropriate oversight to safeguard against misuse. Adhering to these guidelines ensures that AI contributes positively to the educational environment and aligns with BCC's commitment to ethical practices and student wellbeing.

## Network and Internet Use

- The College network and internet resources are valuable tools for learning and communication. All users are responsible for using these resources efficiently and prioritising activities that support educational goals.
- Users must be mindful of data download and upload limitations when accessing online content or engaging in network activity and consider the impact their usage might have on others' access and the overall network performance.
- If users' activities require significant data usage, they should consult with relevant staff to explore options and ensure responsible resource allocation.
- Overloading the network with excessive bandwidth usage, downloading large files for personal use during peak hours, or engaging in activities that disrupt others' access to network resources must be avoided.
- Accessing websites or online services that contain harmful content or present security, and privacy concerns is strictly prohibited.
- Using school network resources for personal gain, such as running commercial businesses or engaging in unauthorised online activities is prohibited.

## Personal Device Use

- Personal devices are covered under the *BCC Student Laptop Policy* and the *BCC Staff Device Agreement*, which require compliance with this policy. Personal devices may only be used for school or work purposes with prior permission and under specific guidelines outlined in this policy.
- The College reserves the right to access, review, or destroy any intellectual property (IP) and data that belong to the College, regardless of where they are stored, including personal devices. This right is established to ensure the protection and proper management of College assets and information, and compliance with College policies and relevant legislation.
- Users are responsible for the security and appropriate use of their personal devices on school premises. The school assumes no responsibility for their loss, theft, or damage.
- Personal device use must not disrupt the learning environment or interfere with school activities.
- Personal devices must not be used to access websites or content prohibited on school technology.

- Recording audio or video with personal devices during school-related activities without the consent of all individuals involved and in contravention to relevant laws and school policies is strictly prohibited.
- Users must not utilise personal email accounts and platforms for school-related communication or storage of school documents, unless for approved purposes. Likewise, users must not use work email accounts for personal communication or storage of documents.

## **Use of School Identity**

- BCC's name, or any images where BCC or BCC students are identifiable, such as students in uniform, may not be used as content to post online without the permission of the College. This includes but is not limited to posting images or video footage on social media sites.
- Use of social media must not impact or damage the reputation of BCC, or any previous/current BCC staff or students.

## **Consequences of Violation**

BCC takes violations of this policy seriously. Misuse of ICT may result in a range of consequences, depending on the severity of the offence. Possible consequences may include:

- Discussions
- Access Restrictions
- Disciplinary Actions
- Legal Consequences

Users must report suspected violations of this policy promptly to [compliance@bcc.net.au](mailto:compliance@bcc.net.au). The Principal or Board can also hand down a consequence in exercising their own judicious discretion.

## **Resources and Support**

BCC will ensure that appropriate information, training, instruction, and supervision are provided to users to enable them to use BCC's ICT assets in accordance with this policy. For technical assistance, users may contact BCC IT Helpdesk Support. Additional resources and information on safe and ethical technology use are available from the relevant learning management systems (LMS).

# Appendix 1: Cybersecurity Guidelines

At Bundaberg Christian College (BCC), maintaining a secure digital environment is essential to protect the confidentiality, integrity, and availability of sensitive information and to mitigate potential risks associated with cyber threats. All users are required to adhere to the following cybersecurity guidelines:

## 1. Password Management:

- Choose strong and unique passwords for all accounts, combining uppercase and lowercase letters, numbers, and special characters.
- Avoid using easily guessable information such as birthdays, names, or common phrases.
- Do not share passwords with anyone, including friends or colleagues.
- Regularly update passwords and avoid reusing them across multiple accounts.
- Enable multi-factor authentication wherever possible to add an extra layer of security.

## 2. Data Protection:

- Handle sensitive data, including personal and financial information, with care and discretion.
- Users **must not** send any sensitive or health information by email attachment.
- Use Office365 (OneDrive) links for secure sharing of documents containing sensitive and health information.
- Keep software and applications up to date with the latest security patches and updates.
- Regularly backup important data and store backups in a secure location.
- Always lock your device when leaving it unattended.

## 3. Safe Browsing Habits:

- Exercise caution when clicking on links or downloading files from unknown or suspicious sources.
- Verify the authenticity of websites before entering personal information or making online transactions.
- Use secure connections (HTTPS) when accessing sensitive websites or transmitting confidential data.
- Avoid accessing sensitive information over public Wi-Fi networks, as they may be vulnerable to interception.

## 4. Email Security:

- Be wary of unsolicited emails, especially those containing suspicious attachments or requesting sensitive information.
- Verify the legitimacy of email senders before responding to requests for personal or financial information.
- **Do not** click on links or download attachments from unknown or untrusted sources.
- Report any suspicious emails, or incidents to the IT department **immediately**.

## 5. Reporting Procedures:

- Promptly report any suspicious activities, potential security breaches, or incidents of cyberbullying to the IT department.
- Provide detailed information about the nature of the incident, including any relevant screenshots, email headers, or logs.
- Cooperate fully with cybersecurity investigations and follow any instructions provided by the IT department to mitigate risks and prevent further incidents.

By following these cybersecurity guidelines, students and staff can contribute to the overall security posture of BCC and help create a safer digital environment for everyone in the College community.

These guidelines are reviewed regularly and communicated effectively to ensure that all members of the college community understand their roles and responsibilities in maintaining cybersecurity.

## **Appendix 2: Acceptable Use of ICT Policy: Student Version**

Welcome to Bundaberg Christian College (BCC)! We're excited to have you as part of our school community. To make sure everyone stays safe and respectful while using technology at BCC, we have some important rules for you to follow. These rules are called the Acceptable Use of ICT Policy, and they help keep our digital environment secure and enjoyable for everyone.

### **Using Devices Responsibly:**

- When using College computers, laptops, tablets, or other devices, remember to treat them with care and respect.
- Only use the devices for school-related activities approved by your teachers or staff.
- Keep your login information, like usernames and passwords, private. Don't share them with anyone else.

### **Be Kind:**

- Always be kind and respectful when communicating with others online, including classmates and teachers.
- Avoid saying or doing anything online that could hurt someone's feelings or make them uncomfortable.
- If you see someone being bullied or treated unfairly online, report it to a teacher or trusted adult right away.
- Apply the THINK acronym when interacting online: **T - It is true, H - Is it honest, I - Is it Inspiring, N - is it Necessary, K - is it Kind?**

### **Protecting Your Personal Information:**

- Never share personal information online, such as your full name, address, phone number, or school details, with people you don't know.
- Be careful when sharing photos or videos online. Make sure they don't reveal too much about you or others.
- Remember nothing online is private, once online you cannot get it back.

### **Using the Internet Safely:**

- Only visit websites that are safe and appropriate for school. If you're not sure if a website is safe, ask a teacher or adult for help.
- Avoid clicking on pop-up ads or downloading files from unknown sources. They could contain viruses or harmful software.

### **Respecting Copyrights:**

- Always give credit to the original creators of content you use online, such as images, videos, or text.
- Don't copy or use other people's work without their permission, unless it's for schoolwork and you've properly cited your sources.

### **Reporting Problems:**

- If you see something online that makes you feel uncomfortable or unsafe, tell a teacher or trusted adult right away.
- Don't be afraid to speak up if you think someone is breaking the rules or being mean online. Your teachers are here to help.

Remember, using technology is a privilege, and with that privilege comes responsibility. By following these rules, you'll help create a positive and safe digital environment for everyone at BCC. If you ever have any questions or need help, don't hesitate to ask your teachers or school staff.